Penilaian Tingkat Keamanan Informasi Dengan Pendekatan Risiko pada Inspection Kendaraan (Studi Kasus: *Certificate of Roadworthiness* di PT. XYZ)

Rita Rijayanti[1)]
Universitas Pasundan
Jl. Setiabudhi No.196, telp/fax of institusi/ afiliasi
e-mail: rita.rijayanti@unpas.ac.id

Abstrak

Seiring dengan berjalannya waktu, perkembangan jaman dan teknologi, kebutuhan akan sharing data dan informasi secara online pun sudah menjadi kebutuhan dasar dalam aktivitas keseharian masyarakat. Dimana setiap orang ataupun organisasi mengharapkan data atau informasi yang mereka butuhkan dapat dihasilkan secara cepat, tepat dan aman, guna menunjang aktifitas kesehariannya. Seperti halnya kasus yang diangkat pada penelitian ini, berkaitan dengan bidang jasa inspection kendaraan dimana dalam kegiatan oprasional-nya berkaitan dengan banyak transaki data yang dilakukan oleh banyak user yang terdapat pada lokasi yang berjauhan. Dengan demikian perusahaan memiliki kebutuhan akan sharing data secara online, khususnya untuk Certificate Of Roadworthines (COR) dari kendaraan-kendaraan yang telah dilakukan inspection oleh perusahaan XYZ yang sifatnya sangat rahasia dan bernilai tinggi. Perusahaan harus dapat menjamin data yang dikelola dan diterima Customer adalah data yang benar dan asli, karena keaslian data sangat penting dalam konsep keamanan informasi. Salah satu cara yang dapat dilakukan untuk memastikan kondisi keamanan data dan informasi adalah dengan melakukan penilaian risiko, yang dimaksudkan untuk memutuskan kendali yang cocok untuk mencegah terjadinya kerusakan ataupun kerugian. Dimana setiap risiko yang ada akan dibagi kedalam tingkatan/level, sehingga dapat diketahui apakah risiko yang ada saat ini masih dapat dikendalikan atau membutuhkan kontrol keamanan. Pada penelitian ini penilaian risiko COR akan dilakukan metode OCTAV Allegro dengan membagi risiko menjadi menjadi 4 level (Extrem, tinggi, moderat, dan rendah) yang didasarkan pada kemungkinan dan dampak dari setiap risiko, sehingga dapat diketahui kondisi keamanan yang ada saat ini, apakah membutuhkan penanganan kontrol keamanan atau tidak.

Kata kunci: *Risiko, Certificate of Roadworthiness, OCTAV Allegro, dan kontrol keamanan.*

1. Pendahuluan

Seiring dengan berjalannya waktu, perkembangan jaman dan teknologi saat ini, menumbuhkan kebutuhan akan sharing data dan informasi secara online yang dirasa menjadi salah satu kebutuhan dasar dalam aktivitas keseharian masyarakat. Dimana setiap orang ataupun organisasi mengharapkan data atau informasi yang mereka butuhkan dapat dihasilkan secara cepat, tepat dan aman, guna menunjang aktifitas kesehariannya. Seperti halnya kasus yang diangkat pada penelitian ini, berkaitan dengan bidang jasa *inspection* kendaraan dimana dalam kegiatan oprasional-nya berkaitan dengan banyak transaki data yang dilakukan oleh banyak user yang terdapat pada lokasi yang berjauhan. Dengan demikian perusahaan memiliki kebutuhan akan sharing data secara online, khususnya untuk pengelolaan *Certificate Of Roadworthines* (COR) dari kendaraan-kendaraan yang telah dilakukan inspection oleh perusahaan XYZ yang sifatnya sangat rahasia dan bernilai tinggi.

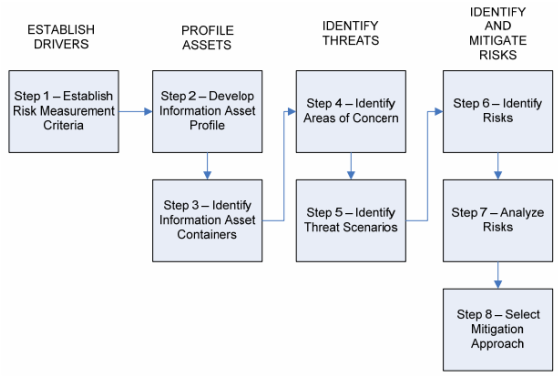
Sejauh ini belum pernah dilakukan analis keamanan informasi pada proses COR di perusahaan XYZ, padahal COR ini sifatnya sangat rahasia dan bernilai tinggi, sehingga seharusnya perusahaan dapat menjamin bahwa data yang dikelola dan diterima *Customer* dalam kondisi aman dalam artian benar dan asli. Karena keaslian data sangat penting dalam konsep keamanan informasi, hal ini dapat menyebabkan turunya kredibilitas dan kepercayaan dari customaer kepada perusahaan. Untuk memastikan kondisi keamanan informasi yang ada, Salah satu cara yang dapat dilakukan untuk memastikan kondisi keamanan data dan informasi adalah dengan melakukan penilaian risiko, yang dimaksudkan untuk memutuskan

kendali yang cocok untuk mencegah terjadinya kerusakan ataupun kerugian. Dimana setiap risiko yang ada akan dibagi kedalam tingkatan/level, sehingga dapat diketahui apakah risiko yang ada saat ini masih dapat dikendalikan atau membutuhkan kontrol keamanan. Pada penelitian ini penilaian risiko COR akan dilakukan metode OCTAV Allegro sehingga dapat diketahui kondisi keamanan yang ada saat ini, apakah membutuhkan penanganan kontrol keamanan atau tidak.

2. Metode Penelitian

Metode yang akan dilakukan pada penelitian ini adalah dengan menggunakan OCTAV allegro, Sebagai metode penilaian dan perencanaan keamanan sistem informasi berbasis risiko (fokus kepada aset informasi) [1]. Dimana pada tahapan awal akan dilakukan penetapan aset, identifikasi risiko dan melakukan analisis risiko, sehingga dapat dihasilkan nilai dari risiko yang ada dan menetapkan penanganan terhadap solusi terbaik. Metode OCTAVE Allegro terdiri dari delapan tahap yang dikelompokkan menjadi empat kategori atau fase, sebagai berikut:

1. Menetapkan apa yang menjadi arahan organisasi,
2. Membuat profil aset yang dimiliki organisasi.
3. Mengidentifikasi ancaman untuk setiap aset informasi dalam konteks wadahnya.
4. Mengidentifikasi dan mitigasi risiko terhadap aset informasi dan pengembangan pendekatan mitigasi.



Gambar 1. Tahapan OCTAV Allegro [1]

Probabilitas		Kriteria
Rating	%	
1	0-10	Sangat tidak mungkin/hampir mustahil
2	10-30	Kecil kemungkinan, tapi tdk mustahil
3	30-50	Kemungkinan terjadi
4	50-90	Kemungkinan Sering terjadi
5	> 90	Hampir pasti terjadi

Gambar 2. Tabel Pengukuran Probabilitas kemunculan [4]

Rating Dampak	Keterangan
Sangat tinggi/ katastropik	Mengancam program dan organisasi serta *stakeholders*. Kerugian sangat besar bagi organisasi dari segi keuangan maupun politis
Besar	Mengancam fungsi program yang efektif dan organisasi. Kerugian cukup besar bagi organisasi dari segi keuangan maupun politis
Menengah/medium	Mengganggu administrasi program. Kerugian keuangan dan politis cukup besar
Kecil	Mengancam efisiensi dan efektivitas beberapa aspek program. Kerugian kurang material dan sedikit mempengaruhi stakeholders
Sangat rendah/ tidak signifikan	Dampaknya dapat ditangani pada tahap kegiatan rutin. Kerugian kurang material dan tidak mempengaruhi stakeholders

Gambar 3. Tabel Pengukuran Dampak dari Risiko [4]

Rumus Risiko [2]:

Risiko = Pobabilitas X Dampak

MATRIKS ANALISIS RISIKO 5X5			Dampak				
			1	2	3	4	5
Deskripsi	Proba-bilitas	*Likeli-hood*	Tidak signifikan	Kecil	Medium	Besar	Katas-tropik
Hampir pasti	90%	5					
Kemungkinan besar	70%	4					
Mungkin	50%	3					
Kemungkinan kecil	30%	2					
Sangat jarang	10%	1					

RATING/STATUS:

Deskripsi	Level	Level dimulai dari status
Ekstrim	5	15
Tinggi	4	10
Moderat	3	5
Rendah	2	3
Rendah	1	1

Gambar 4. Tabel Pengukuran Dampak dari Risiko [4]

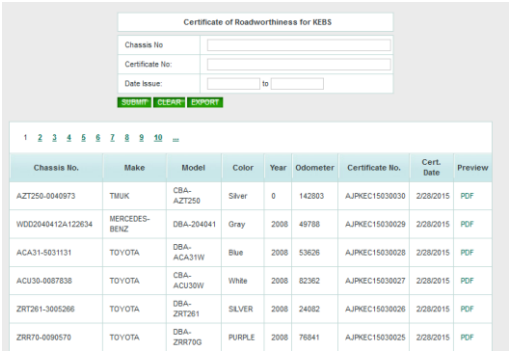
3. Hasil dan Pembahasan

3.1 Analisis

Pada penelitian ini yang menjadi aset adalah data *COR* hasil dari proses *inspection* yang dilakukan oleh perusahaan. Untuk pengelolaan COR dilakukan oleh banyak user, seperti:

1. Sales Team; Pada saat pendaftaran pengajuan inspection dan share data pada Customer. Sales Team hanya dapat melihat dan merubah data status kendaraan pada region masing-masing dengan Customer yang sudah terdaftar pada mereka.
2. Accounting; Bertanggung jawab pada proses pengelolaan pembiayaan inspection dari setiap kendaraan, karena bisa saja setiap kendaraan tidak lolos COR dan harus dilakukan inspection ulang dan ini harus perijinan accounting. Accounting dapat melihat semua data kendaraan, customer dan inspection yang dilakukan dan merubah biaya inspection.
3. Logistic; bagian penyediaan bagi Inspection Team, hanya dapat melihat data kendaraan yang akan dan telah diinspection khusus region masing-masing.
4. Inscpection Team; Team yang melakukan inspection kendaraan dan mengeluarkan certificat dari setiap kendaraan, dan melakukan pengajuan ulang inspection jika memang diperlukan. Team ini hanya dapat mengelola data-data kendaraan yang akan atau telah dia inspection di region masing-masing (merubah data).
5. Quality Assurance (QA); Tim yang melakukan pengecekan data dan sistem. Dimana dapat memiliki hak akses kesetiap sistem yang dimiliki dengan hak akses penuh.

Berikut adalah aplikasi dan gambaran contoh dari *COR* yang dimiliki oleh perusahaan, dimana semua data dapat terbuka jika user telah melakukan verifikasi (login kedalam sistem), dimana user dapat melakukan pencarian data, export data, medownload Cerrtifiacate dan melakukan update data bagi user yang memiliki hak akses:



Gambar 5. Applikasi pengelolaan *Certificate Of Roadworthiness*

Gambar 6. Contoh *Certificate of Roadworthiness*

3.2 Gambaran Umum Data yang Disharing

COR merupakan data yang disharing secara online (website dan dekstop *application*), data yang muncul pada aplikasi selain COR adalah data customer, kendaraan, dan pembiayaan yang dimiliki perusahaan. Kemungkinan ancaman yang dapat muncul adalah pencurian data, modifikasi sampai dengan penghapusan data. Dari aset dan ancaman yang mungkin muncul maka dapat ditetapkan risiko-risiko yang mungkin muncul antara lain:

Tabel 1. Identifikasi Risiko

Aset	Kerentanan	Ancaman	Risiko
Certificate of Roadwothiness	Tidak adanya kebijakan terkait keamanan data: - Aturan terkait peberian hak akses seseorang / bagian. Jika ada yang mengajukan untuk dibukakan hak akses pada DBA, ybs akan langsung membukakan. - Tidak ada pengecekan ulang hak akses ketika karyawan resign.	Kayawan (Sales team, Accounting, Logistik, Inspection Team, dan QA)	1. Manipulasi data. 2. Adanya pencurian data *Certificate of Roadtheness*.
	Pengembangan aplikasi kurang memperhatikan ketentuan konsep keamanan pengembangan perangkat lunak.	Serangan melalui applikasi (SQL Injection, XML injection dll)	
	Pengembang aplikasi yang terpisah-pesah lokasi.	Singkronisasi data pada aplikasi menjadi tidak sesuai requiremen, terkadang peruahan pada satu modul berdampak pada modul yang lain.	3. Kesalahan pengolahan data.

1.3 Hasil Pengelolaan

Berikut ini adalah gambaran hasil penilaian risiko, dimana dari risiko yang telah diidentifikasi, kemudian ditetapkan kemungkinan kemunculan dari setiap risiko rsebut dan dikalikan dengan dampak yang mungkin terjadi:

Tabel 2. Pengolahan Data

Risiko	Probabilitas	Dampak	Nilai Risiko
1. Adanya Manipulasi data COR	2. Kemungkinan sangat kecil manipulasi dilakukan oleh karyawan yang masih berkerja dipeusahaan, namun pernah terjadi walau secara tidak sengaja (rata-rata 1x pebulan - 10%)	1. Kerugian secara finansial bagi perusahaan. 2. Kerugian secara kepercayaan customer kepada perusahaan. 3. Rusaknya nama baik perusahaan.	<u>Oleh karyawan</u> - P 10% = LH 1 - D 5 <u>Non Karyawan</u> - P 70% = LH 4 - D 5
2. Adanya pencurian data *COR*	3. Kemungkinan sangat besar ketika ada karyawan yang keluar dari perusahaan, namun hak akases yang bersangkutan tidak ditutup, dilihat dari tingginya tingkat keluar masuk karyawan perbulan (5 orang perbulan – 70%).		- P 70% = LH 4 - D 5
3. Kesalahan pengolahan data.	4. Adanya pengguna yang mencoba melakukan SQL Injection ataupun manipulasi lainnya (1-2x dalam satu bulan – 50%). 5. Kesalahan pengelolaan data pada modul yang dikembangkan-berkaitan karyawan yang menangani berbeda-beda setiap waktunya dan dilihat (jumlah support yang muncul per pulan bisa mencapai 15x per bulan – 80%)		- P 80% = LH 4 - D 5

*) Nilai Risiko (NR) = Probabilitas (P) x Dampak (D)

Posisi Grafik Nilai Risiko dari hasil pengolahan data, perkalian dari probabilitas –Likelihood dan dampak ditunjukan dengan matrik analisis rasio berikut ini:

MATRIKS ANALISIS RASIO 5x5			DAMPAK				
			1	2	3	4	5
Deskripsi	Peoba-bilitas	Likeli-hood	Tidak Signifikan	Kecil	Medium	Besar	Katas Topik
Hampir Pasti	90%	5					
Kemungkinan Besar	70%	4				1.2, 2, 3	
Mungkin	50%	3					
Kemungkinan Kecil	30%	2					
Sangat Jarang	10%	1				1.1	

RATING/STATUS:

Deskripsi	Level	Level dimulai dari status
Ekstrim	5	15
Tinggi	4	10
Moderat	3	5
Rendah	2	3
Rendah	1	1

Gambar 7. Tabel Pengukuran Dampak dari Risiko

Dari table matrix diatas dapat dilihat bahwa kondisi saat ini masih membutuhkan pengendalian keamanan informasi, karena memiliki rating/setatu extrim seperti pada risiko 1.2, 2 dan 3 yaitu, Manipulasi ,pencurian data COR dan juga risiko kesalahan pengolahan data baik itu yang dilakukan oleh karyawan atau pun bukan.

Jika dilihat kembali, hal ini dapat dikarenakan tidak adanya ketentuan terkait pengamanan data, sampai dengan pengembangan aplikasi yang dirasa masih kurang. Maka kasus pada perusahaan XYZ ini cenderung kepada memerlukan adanya kebijakan keamanan informasi dan pengembangan perangkat lunak yaitu dengan penanganan [2]

4. Kesimpulan dan Saran

4.1 Kesimpulan

Pada perinsipnya penilaian risiko merupakan suatu proses identifikasi terhadap aset informasi, ancaman, dan kerentanan yang dapat dilakukan dengan berbagai metode. Pada penelitian ini penilaian risiko menggunakan metode OCTAV Allegro sebagai metode penilaian dan perencanaan keamanan sistem informasi berbasis risiko (fokus kepada aset informasi). Didapatkan bahwa masih terdapat celah keamanan dengan nilai risiko ekstrim pada pengelolaan data *COR*, dimana data yang ada masih dapat dicuri, dimodifikasi sampai dengan dihapus oleh orang yang tidak bertangung jawab sehingga dapat menyebabkan kerugian bagi perusahaan. Hal ini dikaranakan tidak adanya ketentuan terkait pengamanan data, sampai dengan pengembangan aplikasi yang dirasa masih kurang.

4.2 Saran

Saran dari peneliti perusahaan melakukan perbaikan kebijakan terkait dengan keamanan dalam pengembangan perangkat lunak yang ada di perusahaan tersebut. Melakukan pengelolaan aktif dan review rutin, menetapkan strategi harus dilaksanakan, terutama difokuskan pada pemeliharaan untuk pengendalian keamanan data.

Daftar Pustaka

[1] Caralli, Richard. A. Stevens, James F. Young. Lisa R and Wilson William R. 2007. Introductiong OCTAVE Allegro: Improving the Information Security Risk Assesment Process. US: Carnegie Mellon University.

[2] Iso Copyright Officer. *International Standard ISO/IEC 27001- Information Technology – Security Technique – Information Security Management System - Requirements*. 2013; vol: 2013.

[3] Assessing Risk Probability: Alternative Approaches, PMI Global Congress Proceedings – Prague, Czech Republic. http://www.risk-doctor.com/pdf-files/hha0404.pdf, accessed October 15, 2013.

[4] SPIP. Penilaian Risiko. 2011.

[5] Rita Rijayanti. Perancangan Kontrol Keamanan Teknologi Informasi Berdasarkan Penilaian Risiko Selama Siklus Hidup Pengembangan Perangkat Lunak (Studi Kasus di PT. XYZ). Bandung – Universitas Langlangbuana. 2015.